Cybersecurity for Distributed Science: Fortifying the Front-lines of the Cybersecurity War

Speaker: Deborah Agarwal, Lawrence Berkeley National Laboratory

Abstract

Scientific discovery has become a global, collaborative endeavor involving access to a broad range of computer resources to complete an experiment, run a simulation, or search databases. For example, each year the DOE Office of Science facilities are used by more than 18,000 researchers from universities, other government agencies, and private industry. The computer used by a researcher to access a remote facility is typically not under the control of the remote facility and so compromise of that computer and its accounts is difficult for the remote facility to detect. Providing access to legitimate remote users while recognizing and rejecting attackers presents an enormous security challenge when the two are not easily differentiated. Protections for high value resources are particularly important because recovery of these resources is expensive and time consuming. For example, recovery of a compromised supercomputer system can take weeks, during which the machine is unavailable for its many users.

In addition, distributed collaborative projects typically form a virtual organization. The virtual organization model redefines the traditional enclave into one that crosses and incorporates several site borders and includes personnel and resources from a wide range of sites. These virtual organizations often control the fine-grained authentication, authorization, and resource allocation within the collaboration. They need new cyber security tools which enable them to work with sites to monitor and protect against improper use of the resources of the virtual organization.

In today’s environment the components of a cybersecurity system include all the traditional network-based cybersecurity mechanisms, the operating system protections, and the middleware authentication/authorization mechanisms. Deployment of each component in such a cybersecurity system is a balance between cost and benefit. The cost calculation includes not only the equipment but also the staff time required to configure, install, and monitor the component. Decisions regarding which components are needed and where at a particular enclave are typically determined locally based on risk analysis and an expected return-on-investment (ROI) calculation. Reducing the overall cost while improving the effectiveness of cybersecurity should be a priority.

This talk will focus on some practical solutions needed for the cybersecurity and infrastructure challenges facing enclaves today. These challenges include: protecting high performance networking and computing environments, providing distributed computing and access while protecting resources, coordinating between cybersecurity components to recognize and react to cyber threats, integration of middleware security mechanisms into the enclave cybersecurity approach, reducing the human cost of effective cybersecurity, and implementation of improved authentication mechanisms in the environment.